OFFICE OF THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

RISKS POSED BY DIGITAL PHOTOCOPIERS USED IN SOCIAL SECURITY ADMINISTRATION OFFICES

September 2008 **A-06-08-28076**

AUDIT REPORT

Mission

By conducting independent and objective audits, evaluations and investigations, we inspire public confidence in the integrity and security of SSA's programs and operations and protect them against fraud, waste and abuse. We provide timely, useful and reliable information and advice to Administration officials, Congress and the public.

Authority

The Inspector General Act created independent audit and investigative units, called the Office of Inspector General (OIG). The mission of the OIG, as spelled out in the Act, is to:

- **Conduct and supervise independent and objective audits and investigations relating to agency programs and operations.**
- **Promote economy, effectiveness, and efficiency within the agency.**
- **Prevent and detect fraud, waste, and abuse in agency programs and operations.**
- **Review and make recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.**
- **Keep the agency head and the Congress fully and currently informed of problems in agency programs and operations.**

To ensure objectivity, the IG Act empowers the IG with:

- **Independence to determine what reviews to perform.**
- **Access to all information necessary for the reviews.**
- **Authority to publish findings and recommendations based on the reviews.**

Vision

We strive for continual improvement in SSA's programs, operations and management by proactively seeking new ways to prevent and deter fraud, waste and abuse. We commit to integrity and excellence by supporting an environment that provides a valuable public service while encouraging employee development and retention and fostering diversity and innovation.

SOCIAL SECURITY

MEMORANDUM

Date: September 18, 2008 Refer To:

To: The Commissioner

From: Inspector General

Subject: Risks Posed by Digital Photocopiers Used in Social Security Administration Offices (A-06-08-28076)

OBJECTIVES

Our objectives were to (1) determine whether the Social Security Administration (SSA) used digital photocopiers with memories capable of retaining sensitive information and (2) identify and review actions SSA had taken to mitigate the risks posed by the potential exposure of this sensitive information.

BACKGROUND

The *Privacy Act of 1974*[1] provides the framework for regulating the collection, maintenance, use, and dissemination of personal information by Federal executive branch agencies. In particular, the *Privacy Act* requires that each Agency

> . . . establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.[2]

The loss of personally identifiable information (PII) can result in harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. Accordingly, SSA has responsibility under the law to appropriately safeguard sensitive PII, including PII on the hard drives of digital photocopiers. Most digital photocopiers manufactured in the past 5 years have hard drives. Digital photocopier hard drives retain previously copied or printed data. According to SSA staff, when the photocopier hard drive security issue first surfaced, the copier industry did not generally recognize the potential security risks associated with the memory retention capability of photocopier hard drives. SSA followed the industry's lead on this

[1] The *Privacy Act of 1974*, as amended, Pub. L. No. 93-579, 5 United States Code (U.S.C.) § 552a.

[2] 5 U.S.C. § 552a(e)10.

issue. Now, photocopiers have emerged as intelligent system peripherals with operating systems, hard drives, resident software programs and network server applications. Left unprotected or unaccounted for, digital technology can increase the potential for identity theft.

The Office of Acquisition and Grants (OAG) delegated sole acquisition authority to the Office of Publications and Logistics Management, Reprographic Management Team (RMT) to procure and manage reprographic equipment (photocopiers), services, and supplies for all SSA Regional and Headquarters offices nationwide. With OAG approval, RMT established 12 active Blanket Purchase Agreements (BPA) covering reprographic equipment purchase, supplies, and maintenance services. As of December 2007, RMT records indicated SSA had 4,663 photocopiers in use. The inventory included 97 different photocopier models manufactured by 7 vendors.

RESULTS OF REVIEW

As of December 2007, 2,173 of the 4,663 photocopiers SSA had in-use nationwide contained hard drives capable of retaining sensitive information. We found that SSA did not effectively mitigate the risks posed by the potential exposure of sensitive information.[3] During our review, we found SSA did not

- sanitize or destroy photocopier hard drives upon disposal, as required, and
- include a non-disclosure statement in its agreement with vendors that precludes the disclosure of sensitive information when photocopiers are taken off-site for repair.

Additionally, SSA's inventory tracking system did not adequately (1) distinguish between stand-alone photocopiers with no hard drives and photocopiers with hard drives or (2) account for purchases in a timely manner.

SSA DID NOT SANITIZE PHOTOCOPIER HARD DRIVES BEFORE DISPOSITION

SSA did not comply with policy for sanitizing or destroying data stored on hard drives upon disposal. For example, when SSA replaces a photocopier, a vendor delivers the new photocopier and picks up the old photocopier at its respective location. SSA does not sanitize or destroy information on the old photocopier's hard drive before releasing it to the vendor. As depicted in the table below, in Calendar Years 2006 and 2007, SSA traded in 1,957 photocopiers on the purchase of new photocopiers. We found 454 of the 1,957 photocopiers had hard drives.

[3] We are not aware of any reported cases of PII breach involving digital photocopiers.

RMT Copier Trade-Ins (Calendar Years 2006-2007)		
With Hard Drives	454	23.2%
Other	1,503	76.8%
Total	**1,957**	**100.0%**

SSA did not have procedures in place to ensure that photocopier hard drives were sanitized or destroyed. We were told the responsibility for sanitizing or destroying photocopier hard drives had not been assigned within SSA or contracted to an outside entity.

SSA's Information Systems Security Handbook (ISSH) requires that hard drives be sanitized before they are released to a vendor to prevent unauthorized disclosure of information.[4] However, at the time of our review, SSA had not implemented procedures to ensure photocopier hard drives were sanitized or destroyed. While there have been no known unauthorized security breaches, there is a risk of exposing sensitive information to unauthorized individuals.

NON-DISCLOSURE STATEMENT MISSING FROM SERVICE AGREEMENT

SSA did not comply with its own policy to mitigate the risks posed by the potential exposure of sensitive information in the event a photocopier is sent off-site for repair. SSA's BPA does not include required wording for non-disclosure of information by the servicing vendor when a photocopier with a hard drive is repaired off-site. The typical wording related to off-site repairs observed on the BPAs states only the following.

> The Contractor may perform repair work at the Government site, or at the Contractor's local service branch. If the Contractor removes the equipment for repair, the Contractor shall provide a comparable loaner machine to the Government for temporary use at the time the Contractor removes the equipment for repair.

SSA's BPAs should be updated to reflect SSA's policy on the disposal of information technology media, which went into effect in 2006. The policy states, when a personal computer, hard drive, or other storage device is sent off-site for repair, the repair contract must include a requirement for non-disclosure of information by the servicing vendor.[5] According to RMT staff, the current SSA policy in the ISSH regarding disposal of technology media applies to photocopiers as well.

---

[4] Information Systems Security Handbook 10.3.1, Disposal/Donation of Information Technology Equipment, June 2006. Although the policy does not specify photocopiers, SSA officials advised us the policy applies to photocopier hard drives.

[5] *Id.*

The approved dates of the BPAs reviewed ranged from September 17, 2001 to December 22, 2005, a time period that preceded this 2006 policy. When the disposal of technology media policy was issued in 2006, RMT continued to order reprographic equipment from existing BPAs established by OAG before the 2006 security policy change.

On June 18, 2008, we were advised that SSA was negotiating with all current BPA holders to include language that hard drive sanitation must be completed in instances where photocopiers are (1) sent off-site for repair or when hard drives need to be replaced, (2) relocated to different work sites, and (3) traded in for new photocopiers. In addition, we were advised that RMT requested BPA modifications that will require vendors to complete and submit a hard drive certification form that they have wiped or destroyed the hard drive. Certain vendors can certify the presence of an automatic overwrite feature for certain models that automatically wipes the information from the hard drive. Completion of the form is required for each copier before the removal of SSA's copiers from Regional or Headquarters offices for any reason (repair, relocation or replacement). RMT will retain a copy of each hard drive certification form while the copier remains in service at SSA.

SSA'S PHOTOCOPIER INVENTORY TRACKING SYSTEM

RMT staff track photocopier inventory on Microsoft Excel spreadsheets. During our review, we determined SSA's photocopier inventory tracking system did not adequately

- identify whether photocopiers contained hard drives, and
- track photocopier purchases in a timely manner.

Hard Drives in Photocopiers Not Properly Identified

SSA's system for tracking photocopiers with hard drives requires improvement. Instead of relying on photocopier purchase documents, which record whether each photocopier contained a hard drive, SSA relied on vendors to determine whether the photocopier had a hard drive. Since hard drives were optional on some photocopier models, the reliance on vendors for hard drive information was not always accurate. To illustrate, using RMT's December 2007 inventory data, we identified three photocopier models where the inventory showed the photocopiers did not contain hard drives. Through review of acquisition documentation, we determined hard drives were included on 269 of these photocopiers. Based on our review, RMT updated its inventory data to indicate these 269 photocopiers contained hard drives.[6]

[6] RMT updated its inventory to include one additional photocopier originally purchased without a hard drive but later upgraded with a hard drive.

RMT Photocopier Inventory Data (December 2007)			
Pre-Audit		**Post-Audit**	
Type	**# of Units**	**Type**	**# of Units**
With Hard Drives	1,903	With Hard Drives	2,173
Other	2,760	Other	2,490
Total	**4,663**	**Total**	**4,663**

We believe the system used to track photocopiers should be automated and accurately identify the machines that contain hard drives. To automate its photocopier inventory management and billing process, SSA entered into a contract in September 2007 for an automated inventory system. SSA previously attempted to automate the inventory process. In September 2002, SSA awarded a contract to redesign the RMT photocopier inventory and vendor billing reconciliation processing system, which was named the Reprographic Inventory Management System. In 2003, modifications were issued to the contract, but the contract period expired before the work was completed.

Based on the statement of work under the 2007 contract award, the contractor will migrate the current inventory into an upgraded version of the Office of Property Management's Sunflower Assets system.

Purchases Not Added to Inventory Timely

SSA did not record photocopier purchases in a timely manner. According to SSA, employees track photocopier inventory on Microsoft Excel spreadsheets. However, SSA did not add new inventory to the spreadsheets until the end of each photocopier's 90-day warranty period. We were told newly purchased photocopiers were not added to the inventory because RMT did not always know the serial number. By the end of the warranty period, the serial number had been received from the vendor. By not tracking purchases until the end of the 90-day warranty, there is a 3-month time period where the accounting of photocopiers is incomplete because newly purchased photocopiers are not included on the inventory.

CONCLUSIONS AND RECOMMENDATIONS

SSA uses more than 2,100 digital photocopiers with memories capable of retaining sensitive information and can take steps to mitigate the information security risks posed by digital photocopiers. We determined that SSA had a documented policy to sanitize or destroy information contained on hard drives; however, SSA had not applied the policy to digital photocopiers. For example, SSA traded-in old photocopiers to vendors without SSA sanitizing or destroying information on their hard drives. Also, agreements between SSA and vendors did not include the required non-disclosure language. We also found SSA's inventory did not always accurately identify photocopiers with hard drives or account for photocopiers within a reasonable period. To ensure that SSA fully complies with Federal law and Agency policy, as well as ensure that SSA adequately accounts for its photocopier inventory, we recommend SSA:

1. Establish procedures for sanitizing or destroying photocopier hard drives.

2. Amend the maintenance provision in current BPAs and in future agreements to include the required non-disclosure statement by the servicing vendor when the photocopier is sent off-site for repair.

3. Implement an automated photocopier inventory system that includes the capability of tracking the existence of hard drives.

4. Record all digital photocopier purchases to the automated tracking system within a reasonable time after the equipment is received and installed.

AGENCY COMMENTS

SSA agreed with our recommendations. The full text of the Agency's comments is included in Appendix C.

Patrick P. O'Carroll, Jr.

Appendices

APPENDIX A – Acronyms

APPENDIX B – Scope and Methodology

APPENDIX C – Agency Comments

APPENDIX D – OIG Contacts and Staff Acknowledgments

Acronyms

BPA	Blanket Purchase Agreement
ISSH	Information Systems Security Handbook
OAG	Office of Acquisition and Grants
PII	Personally Identifiable Information
Pub. L. No.	Public Law Number
RMT	Reprographic Management Team
SSA	Social Security Administration
U.S.C.	United States Code

Scope and Methodology

To accomplish our objectives, we

- Reviewed the applicable sections of the *Privacy Act of 1974*, *Federal Information Security Management Act of 2002*, Federal Acquisition Regulations, Social Security Administration's (SSA) Program Operations Manual System, Administrative Instructions Manual System and Information Systems Security Handbook.

- Considered the security implications of Office of Management and Budget Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information*, July 12, 2006.

- Interviewed SSA employees from the Center for Office Property, Office of Acquisition and Grants, and Office of Information Technology Security Policy.

- Obtained a database of photocopiers in use nationwide. We performed limited testing on the data and found them to be sufficiently reliable to meet our audit objectives.

- Selected and reviewed six photocopier models with hard drives on SSA's database. These 6 models totaled 1,626 (75 percent) of the 2,173 inventoried photocopiers with hard drives.

- Obtained a database of photocopiers traded in for new photocopiers in Calendar Years 2006 and 2007.

We performed audit work between December 2007 and May 2008 in Baltimore, Maryland, and Dallas, Texas. The entity audited was SSA's Office of Publications and Logistics Management under the Deputy Commissioner for Budget, Finance and Management. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Agency Comments

SOCIAL SECURITY

MEMORANDUM

Date: September 3, 2008 Refer To: S1J-3

To: Patrick P. O'Carroll, Jr.
Inspector General

From: David V. Foster /s/ J. Winn for DVF
Executive Counselor to the Commissioner

Subject: Office of the Inspector General (OIG) Draft Report, "Risks Posed by Digital Photocopiers Used in Social Security Administration Offices" (A-06-08-28076)--INFORMATION

We appreciate OIG's efforts in conducting this review. Attached is our response to the recommendations.

Please let me know if we can be of further assistance. Please direct staff inquiries to Ms. Candace Skurnik, Director, Audit Management and Liaison Staff, at (410) 965-4636.

Attachment

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL (OIG) DRAFT REPORT, "RISKS POSED BY DIGITAL PHOTOCOPIERS USED IN SOCIAL SECURITY ADMINISTRATION OFFICES" (A-06-08-28076)

Thank you for the opportunity to review and provide comments on this draft report.

Recommendation 1

Establish procedures for sanitizing or destroying photocopier hard drives.

Comment

We agree. In November 2007, we began efforts to incorporate a hard drive sanitization policy into all photocopier purchase and maintenance Blanket Purchase Agreements (BPA). We included statements in the BPAs addressing sanitizing hard drives for all trade-ins. In July 2008, we began processing procurements with the hard drive sanitization requirements. We require each vendor to complete a hard drive certification form and instruction sheet certifying that each photocopier with a hard drive has automatic hard drive overwrite capability or that the contractor has erased/destroyed all data on the hard drive for each photocopier model.

By December 30, 2008, we will amend the Administrative Instructions Manual System (AIMS) guidelines and post updated policies to our website at http://ssahost.ba.ssa.gov/oplm/default.cfm.

Recommendation 2

Amend the maintenance provision in current BPAs and in future agreements to include the required non-disclosure statement by the servicing vendor when the photocopier is sent off-site for repair.

Comment

We agree. We amended all current maintenance BPAs to include a requirement specifying that the contractor must overwrite (wipe) or destroy all data on the hard drive and certify this information on a hard drive certification form each time a photocopier is removed from our premises for any reason. In June 2008, the vendors signed the BPA modifications. We also added this new requirement for all future Statements of Work requesting vendor bids.

The hard drive security provisions will be included in all future maintenance agreements. By December 30, 2008, we will amend the AIMS guidelines and post the updated policies to our website at http://ssahost.ba.ssa.gov/oplm/default.cfm.

Recommendation 3

Implement an automated photocopier inventory system that includes the capability of tracking the existence of hard drives.

Comment

We agree. In September 2007, we awarded a contract to Annams, Inc., to create an automated inventory management system to track photocopiers. The new system will be a module of our existing Sunflower Assets system. In June 2008, Annams completed a prototype demonstration. On August 19, 2008, we delivered to Annams all photocopier data for migration into the new inventory management system. The data files for migration will include hard drive information for each photocopier. September 30, 2008, is our target date for completing the new automated system. However, all photocopiers are now manufactured to include hard drives and while we agree with the recommendation for existing copiers, we believe it will be unnecessary to specifically track the existence of hard drives of copiers purchased in the future.

Recommendation 4

Record all digital photocopier purchases to the automated tracking system within a reasonable time after the equipment is received and installed.

Comment

We agree. We have already incorporated language in current BPAs addressing the reporting requirement for contractors providing photocopiers to us. This procedure includes our newly created Proof of Install (POI) form for all new photocopier installations. The vendor must complete the form and obtain our signature at the installation site. The vendor must submit the form to us by the 15th of the month following installation. The POI form will be included in all future copier agreements as a requirement under delivery and installation procedures. As cited above, our photocopier inventory system scheduled to be operational in September 2008 will allow us to upload delivery and installation data to the automated system in a timely manner.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Ron Gunia, Director, (214) 767-6620

Jason Arrington, Audit Manager, (214) 767-1321

Acknowledgments

In addition to those named above:

Lela Cartwright, Senior Auditor

For additional copies of this report, please visit our web site at www.ssa.gov/oig or contact the Office of the Inspector General's Public Affairs Staff Assistant at (410) 965-4518. Refer to Common Identification Number A-06-08-28076.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget, Income Maintenance Branch

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

Chairman and Ranking Minority Member, Committee on the Budget, House of Representatives

Chairman and Ranking Minority Member, Committee on Oversight and Government Reform

Chairman and Ranking Minority Member, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority Member, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Committee on Finance

Chairman and Ranking Minority Member, Subcommittee on Social Security Pensions and Family Policy

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of an Office of Audit (OA), Office of Investigations (OI), Office of the Counsel to the Inspector General (OCIG), Office of External Relations (OER), and Office of Technology and Resource Management (OTRM). To ensure compliance with policies and procedures, internal controls, and professional standards, the OIG also has a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts financial and performance audits of the Social Security Administration's (SSA) programs and operations and makes recommendations to ensure program objectives are achieved effectively and efficiently. Financial audits assess whether SSA's financial statements fairly present SSA's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs and operations. OA also conducts short-term management reviews and program evaluations on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts investigations related to fraud, waste, abuse, and mismanagement in SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, third parties, or SSA employees performing their official duties. This office serves as liaison to the Department of Justice on all matters relating to the investigation of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Counsel to the Inspector General

OCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCIG also advises the IG on investigative procedures and techniques, as well as on legal implications and conclusions to be drawn from audit and investigative material. Also, OCIG administers the Civil Monetary Penalty program.

Office of External Relations

OER manages OIG's external and public affairs programs, and serves as the principal advisor on news releases and in providing information to the various news reporting services. OER develops OIG's media and public information policies, directs OIG's external and public affairs programs, and serves as the primary contact for those seeking information about OIG. OER prepares OIG publications, speeches, and presentations to internal and external organizations, and responds to Congressional correspondence.

Office of Technology and Resource Management

OTRM supports OIG by providing information management and systems security. OTRM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OTRM is the focal point for OIG's strategic planning function, and the development and monitoring of performance measures. In addition, OTRM receives and assigns for action allegations of criminal and administrative violations of Social Security laws, identifies fugitives receiving benefit payments from SSA, and provides technological assistance to investigations.